Claims: Applicant requests cancellation of claims 20-35 of record and substitution of new claims 40-55 as follows, leaving claims 36-39 without amendment per the notice filed herewith:

40. A method of electronically signing an electronic transaction record, document, filing, message, binary file or other digital information (hereinafter collectively referred to as "a document" or "the document"), comprising:

a. under control of a client system,

1. sending a client user identifier to a server system;

2. establishing a document to be signed by the server system; and

3. displaying a choice of actions to be taken by the user to confirm an intent to sign the document using an encryption device of the server as an act of signature by the user of the client system; and

b. under control of the server system,

1. controlling access by clients to the server on the basis of client identifiers;

2. electronically signing the document and its identifier using an encryption device stored on the server system upon command by the client user; and

3. with an encryption device stored on the server system, verifying to a relying party the unchanged message contents of an electronically document previously signed using the server and the identity of the client user on whose behalf it was signed.

whereby the document is both electronically signed on behalf of a client user and verified by a relying party using the server computer, without any client-side encryption keys distributed to any signing or relying party, or a need for interoperability of keys, certification authorities, or other methods of identifying users to individual keys in their possession.

B1 cont

41. The method of claim 40 wherein the server computer used for signing generates a unique identifier for the document to be signed that includes a sequence of a combination of one or more computer network location identifiers, together with a reference to the client side identifier of the person or entity on whose behalf signing occurs, and the current date and time as reported by the server's clock.

42. The method of claim 40 wherein the method of the server system to authenticate a user requires a client user to supply a biometric identifier to the server system.

43. The method of claim 41 wherein the server system:

    1. stores each unique document identifier in a database at or accessible to the server as a record of each signature transaction;

    2. at the request of a client side user or a relying party, queries one or more of a collection of unique document identifiers at the server system; and

    3. retrieves and displays, on the basis of each particular unique document identifier supplied, related records to the client side user or relying party, containing information about a signed document, including information about the person or entity on whose behalf a signature was made.

44. The method of claim 40 wherein the actions of a user to sign and confirm an intent to sign are effectuated through voice commands.

45. The method of claim 41 wherein a unique document identifier includes an approval code generated by a credit card payment system and transmitted to the server computer prior to signing on behalf of a credit card user.

46. The method of claim 40 wherein a client side signature device is used to resign the electronic document as a final act of signature intent.

B1 Cont

47. The method of claim 40 wherein the client system user is an electronic process or agent.

48. The method of claim 40 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using the unique document identifier of a document as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes its signature.

49. The method of claim 40 wherein the method of the server system to authenticate a user requires the client user to demonstrate knowledge of a secret,

whereby a username and passphrase, username and password, or personal identification number or other knowledge based system can be used to control access by a client user to a server's signature device, but excluding authentication based on local domain security services on a client–server network with public-key or Kerberos authentication and key establishment.

50. A method of electronically signing an electronic transaction record, document, filing, message, binary file or other digital information (hereinafter collectively referred to as "a document" or "the document"), comprising:

(a) providing a signature encryption means at a server computer,

(b) providing a means of identifying a user,

(c) providing an authentication means of access control for determined classes of users, based upon the permissible means of identifying users.

B1 cont

(d) providing a document template, with spaces to be filled in with character input by a client user,

(e) providing a character input means by which the client user can remotely provide, and as appropriate, review and correct a series of characters that are to be inserted at spaces within a template, in order to assemble a document that includes specific information furnished by the client user,

(f) providing a means for establishing a unique identifier for the document to be signed which includes an identifier of the client user and the current date and time of the server's system clock,

(g) providing a means by which said client user remotely causes the encryption device to affix an electronic signature to the particular document and identifier that was assembled,

whereby documents are created and signed by users using one or more templates and encryption devices located at a remote server over a computer network, including the Internet

51. The method of claim 50 wherein the document to be signed includes formatting tags or codes,

whereby the document can be read by applications that employ such tags or codes after completion and signature.

52. The method of claim 50 wherein the document to be signed includes server-supplied text or graphical information that is displayed to the client user but cannot be modified or deleted by the user,

whereby signature by the client user indicates acceptance and agreement to the supplied text and graphical information as part of the signed document information.

B1 cont

53. The method of claim 50 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using the unique document identifier of a document as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes its signature.

54. The method of claim 50 wherein the actions of a user to sign and confirm an intent to sign are effectuated through voice commands.

55. The method of claim 50 wherein the signed document consists of an envelope for the transmission and routing of other files, each of which is included in or attached to the signed envelope and any or all of which is independently signed using the methods of this invention.

REMARKS -- General

The office action dated March 12, 2001 deemed the amendments and remarks contained in the previous submissions by Applicant moot based upon a single new and supplementary prior art reference enclosed by Applicant with the previous submission. The prior art reference was taken from a book by Baum and Ford entitled "Secured Electronic Transaction". In that reference at pages 332-3, the authors cited as an example in the context of a discussion of non-repudiation the case where a trusted third party digitally signs a message using asymmetric encryption on behalf of originators whose messages are properly authenticated to the server. As